UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/743,784	12/24/2003	Harold J. Johnson	201371-05000	6160

26123 7590 08/19/2009

BORDEN LADNER GERVAIS LLP
Anne Kinsman
WORLD EXCHANGE PLAZA
100 QUEEN STREET SUITE 1100
OTTAWA, ON K1P 1J9
CANADA

EXAMINER	
LOUIE, OSCAR A	

ART UNIT	PAPER NUMBER
2436	

NOTIFICATION DATE	DELIVERY MODE
08/19/2009	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

ipinfo@blgcanada.com

Office Action Summary	Application No.	Applicant(s)	
	10/743,784	JOHNSON ET AL.	
	Examiner	Art Unit	
	OSCAR A. LOUIE	2436	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *22 April 2009*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,31-34,36 and 37* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,31-34,36 and 37* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

This final action is in response to the amendment filed on 04/22/2009. Claims 1, 31-34, 36, & 37 are pending and have been considered as follows.

Specification

1. The specification is objected to as failing to provide proper antecedent basis for the claimed subject matter. See 37 CFR 1.75(d)(1) and MPEP § 608.01(o). Correction of the following is required:

- Claim 1 recites "without otherwise storing said biometric template on said device" which appears to lack antecedent basis from the applicants' Specification.

Claim Objections

2. Claim 1 is objected to because of the following informalities:

- Claim 1 lines 22-24 recite "such that said biometric template is not stored on said device in a form that is accessible without executing said TRS encoded access software application" which should be rephrased to avoid "negative claim" issues;
- For example the applicants can rewrite this claim limitation to read more clearly, "said biometric template is stored on said device in a form that is accessible only through the execution of said TRS encoded access software application" or "said biometric template

is stored on said device in an encrypted form that is accessible only through the execution of said TRS encoded access software application";

Appropriate correction is required.

Claim Rejections - 35 USC § 112

3. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

4. Claim 1 is rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention.

- Claim 1 recites "without otherwise storing said biometric template on said device" which appears to lack support from the applicants' original disclosure.

5. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

6. Claim 1 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

- Claim 1 lines 8-9 recite "without otherwise storing said biometric template on said device" which appears the applicants meant one of the following possible interpretations (not limited to since the wording creates a contradiction with subsequent limitations pertaining to the storage of the biometric template):
    - "said biometric template is stored on the device in an encrypted form"
    - "said biometric template is stored as characteristics of the biometric signature data" (i.e. not the image signatures themselves but a shortened representation of the entire biometric data – see Specification page 24 para 127);
    - "said biometric template is encrypted and customized by the TRS software so that it cannot be used anywhere other than on the original device with the original software and it is never transmitted to a server nor does it leave the user's control during normal use, maintaining privacy" (see Specification page 25 para 142);
- The examiner notes that further clarification is required as the current claim language creates a contradiction and is at the very least unclear with respect to the scope of the applicants' claim limitation.

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. Claim 1 is rejected under 35 U.S.C. 103(a) as being unpatentable over Gennaro et al. (US-6317834-B1) in view of Collberg et al. (US-6668325-B1).

Claim 1:

Gennaro et al. disclose a method of biometric verification using an access software application locally stored on a device and configured to access another application, system or other software entity on said device to protect biometric data against spoofing or theft comprising,

- "establishing parameters of the access software application" (i.e. "Each individual 310 seeking enrollment is prompted to provide enrollment data including a biometric sample, a personal identifier and encryption key generation data…It is to be appreciated that the present invention is not limited to storing only the data elements defined by the various embodiments. The record may be comprised of whatever additional encrypted or unencrypted information the system designer deems necessary, which may be more or less information than that described herein") [column 5 lines 49-52, column 6 lines 59-65];

- "generating a biometric template for a user by sampling" (i.e. "At block 18 a biometric model (T=f(S)) is created from the biometric sample (S)") [column 6 lines 30-31];
- "integrating into the access software application by means of partial evaluation, the parameters and the biometric template without otherwise storing said biometric template on said device" (i.e. "An encrypted biometric record 330 is created for each enrolled individual and stored as part of the biometric database 340…It is to be appreciated that the present invention is not limited to storing only the data elements defined by the various embodiments. The record may be comprised of whatever additional encrypted or unencrypted information the system designer deems necessary, which may be more or less information than that described herein") [column 5 lines 52-54 & column 6 lines 59-65];
- "including storing the biometric template in an encoded format that is irreversible" (i.e. "An encrypted biometric record 330 is created for each enrolled individual and stored as part of the biometric database 340…") [column 5 lines 52-54];
- "such that said biometric template is not stored on said device in a form that is accessible without executing said TRS encoded access software application" (i.e. "An encrypted biometric record 330 is created for each enrolled individual and stored as part of the biometric database 340…In block 26 an individual seeking access to the database is prompted for a personal identifier (I). The system will attempt to match the personal identifier (I) with one of the personal identifiers (I) stored in plaintext as a component of each encrypted biometric record…") [column 5 lines 52-54 & column 7 lines 8-50];

- "employing the biometric template which has been integrated into the access software application to evaluate biometric data provided by a user seeking to access the other application, system or software entity to provide an evaluation result which either permits or denies access by the user" (i.e. "…an individual seeking access to the database is prompted for a personal identifier (I)….match the personal identifier (I) with one of the personal identifiers (I) stored in plaintext as a component of each encrypted biometric record…prompted to provide a password (P')…uses the password (P') to create decryption key (k')…encrypted biometric record will be successfully decrypted only if the password (P') is identical to the password (P)…If the decryption is unsuccessful, the individual cannot be verified and his or her authorization status will be declared as "failed", thereby terminating the verification session. Otherwise, if the decryption of the encrypted biometric record is successful, a decrypted biometric model (T) is extracted from the decrypted biometric record at block 40. In block 32, an individual is further prompted to provide a current biometric sample (S')…the provided biometric sample (S') is compared with the decrypted biometric model (T) for statistical equivalence and a statistical equivalence score is generated therefrom…if the score is above some predetermined accept/reject threshold the individuals authorization status is declared as "failed". Otherwise, an acceptable score will result in authorizing the individual 26 access to the database…") [column 7 lines 8-50];

but, they do not explicitly disclose,

- "performing tamper-resistant software (TRS) encoding to the access software application," although Collberg et al. do suggest applying code obfuscation techniques to stored programs, as recited below;
- "the step of performing TRS encoding being performed according to one of the following: prior to the establishing of parameters, whereby one TRS implementation covers multiple platforms and multiple biometric templates," although Collberg et al. do suggest applying code obfuscation techniques including varying degrees of security dependent on the algorithms and transformations used for the desired level of potency, execution time/space, and cost, as recited below;
- "after the establishing of parameters and before generating the biometric template, whereby one TRS implementation covers one platform only and multiple biometric templates," although Collberg et al. do suggest applying code obfuscation techniques including varying degrees of security dependent on the algorithms and transformations used for the desired level of potency, execution time/space, and cost, as recited below;
- "after the establishing of parameters and after generating the biometric template, whereby one TRS implementation covers one platform only and one biometric template only," although Collberg et al. do suggest applying code obfuscation techniques including varying degrees of security dependent on the algorithms and transformations used for the desired level of potency, execution time/space, and cost, as recited below;

however, Collberg et al. do disclose,

- "Deobfuscation also resembles partial evaluation. A partial evaluator splits a program into two parts: the static part which can be precomputed by the partial evaluator, and the dynamic part which is executed at runtime. The dynamic part would correspond to our original, unobfuscated, program. The static part would correspond to our bogus inner program, which, if it were identified, could be evaluated and removed at deobfuscation time" [column 31 lines 46-53];
- "an unobfuscated program P (e.g., an application), stored in memory 140, can be obfuscated by an obfuscator executing on CPU 130 to provide an obfuscated program P', stored in memory 140, in accordance with one embodiment of the present invention" [column 5 lines 19-24];
- "FIG. 6 shows an architecture of Kava, the Java obfuscator. The main input to the tool is a set of Java class files and the obfuscation level required by the user. The user may optionally provide files of profiling data, as generated by Java profiling tools. This information can be used to guide the obfuscator to make sure that frequently executed parts of the application are not obfuscated by very expensive transformations. Input to the tool is a Java application, given as a set of Java class files. The user also selects the required level of obfuscation (e.g., potency) and the maximum execution time/space penalty that the obfuscator is allowed to add to the application (the cost)" [column 10 lines 57-67 & column 11 line 1];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "performing tamper-resistant software (TRS) encoding to the access software application" and "the step of performing TRS encoding being performed according to one of the following: prior to the establishing of parameters, whereby one TRS implementation covers multiple platforms and multiple biometric templates" and "after the establishing of parameters and before generating the biometric template, whereby one TRS implementation covers one platform only and multiple biometric templates" and "after the establishing of parameters and after generating the biometric template, whereby one TRS implementation covers one platform only and one biometric template only," in the invention as disclosed by Gennaro et al. for the purposes of providing various degrees of security through software code obfuscation of the application that handles biometric enrollment and authentication.

9. Claims 31, 33-34, & 36 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gennaro et al. (US-6317834-B1) in view of Collberg et al. (US-6668325-B1) and in further view of Kaliski, Jr. (US-6085320-A).

Claim 31:

Gennaro et al. and Collberg et al. disclose a method of biometric verification using an access software application locally stored on a device and configured to access another application, system or other software entity on said device to protect biometric data against spoofing or theft, as in Claim 1 above, but their combination do not explicitly disclose,

- "the evaluation result comprises a cryptographic key generated to be either correct to permit access by the user or incorrect to deny access by the user," although Kaliski, Jr. does suggest utilizing a well known protocol for proving authenticity involving keys, as recited below;
- "the cryptographic key being generated to be correct only when the user-provided biometric data is found to match the biometric template," although Kaliski, Jr. does suggest public key/private key, as recited below;

however, Kaliski, Jr. does disclose,

- "A standard well known protocol for proving authenticity involves public-key cryptography. The client establishes a public key/private key pair and provides the public key to the server. In a transaction, to prove its authenticity to the server, the client forms a digital signature with its private key on a time-varying message, and the server verifies the digital signature with the client's public key. The time-varying message, which may be a timestamp or a challenge supplied by the server, is different in each instance. This message, when checked by the server, provides safeguards against a third party impersonating the client by simply replaying copies of previous signatures of the client that the third party has intercepted or otherwise acquired" [column 1 lines 24-36];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "the evaluation result comprises a cryptographic key generated to be either correct to permit access by the user or incorrect to deny access by the user"

and "the cryptographic key being generated to be correct only when the user-provided biometric data is found to match the biometric template," in the invention as disclosed by Gennaro et al. and Collberg et al. for the purposes of providing additional security through key encryption.

Claim 33:

Gennaro et al., Collberg et al., and Kaliski, Jr. disclose a method of biometric verification using an access software application locally stored on a device and configured to access another application, system or other software entity on said device to protect biometric data against spoofing or theft, as in Claim 31 above, but the combination of Gennaro et al. and Collberg et al. do not explicitly disclose,

- "the evaluation result comprises a key for a symmetric cipher having high entropy for its key length, if the user-provided biometric data is found to match the biometric template," although Kaliski, Jr. does suggest public key/private key encryption, as recited below;

however, Kaliski, Jr. does disclose,

- "A standard well known protocol for proving authenticity involves public-key cryptography. The client establishes a public key/private key pair and provides the public key to the server. In a transaction, to prove its authenticity to the server, the client forms a digital signature with its private key on a time-varying message, and the server verifies the digital signature with the client's public key. The time-varying message, which may be a timestamp or a challenge supplied by the server, is different in each instance. This message, when checked by the server, provides safeguards against a third party impersonating the client by simply replaying copies of previous signatures of the client that the third party has intercepted or otherwise acquired" [column 1 lines 24-36];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "the evaluation result comprises a key for a symmetric cipher having high entropy for its key length, if the user-provided biometric data is found to match the biometric template," in the invention as disclosed by Gennaro et al. and Collberg et al. for the purposes of providing additional security through public key/private key encryption.

Claim 34:

Gennaro et al., Collberg et al., and Kaliski, Jr. disclose a method of biometric verification using an access software application locally stored on a device and configured to access another application, system or other software entity on said device to protect biometric data against spoofing or theft, as in Claim 31 above, but the combination of Gennaro et al. and Collberg et al. do not explicitly disclose,

- "the evaluation result comprises private key of a public/private key pair, if the user-provided biometric data is found to match the biometric template," although Kaliski, Jr. does suggest public key/private key encryption, as recited below;

however, Kaliski, Jr. does disclose,

- "A standard well known protocol for proving authenticity involves public-key cryptography. The client establishes a public key/private key pair and provides the public key to the server. In a transaction, to prove its authenticity to the server, the client forms a digital signature with its private key on a time-varying message, and the server verifies the digital signature with the client's public key. The time-varying message, which may be a timestamp or a challenge supplied by the server, is different in each instance. This message, when checked by the server, provides safeguards against a third party

impersonating the client by simply replaying copies of previous signatures of the client that the third party has intercepted or otherwise acquired" [column 1 lines 24-36];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "the evaluation result comprises private key of a public/private key pair, if the user-provided biometric data is found to match the biometric template," in the invention as disclosed by Gennaro et al. and Collberg et al. for the purposes of providing additional security through public key/private key encryption.

Claim 36:

Gennaro et al., Collberg et al., and Kaliski, Jr. disclose a method of biometric verification using an access software application locally stored on a device and configured to access another application, system or other software entity on said device to protect biometric data against spoofing or theft, as in Claim 31 above, but the combination of Gennaro et al. and Collberg et al. do not explicitly disclose,

- "the incorrect cryptographic key is identical in bit-length to the correct cryptographic key," although Kaliski, Jr. does suggest utilizing public key/private key encryption with a time varying message and digital signature, as recited below;

however, Kaliski, Jr. does disclose,

- "A standard well known protocol for proving authenticity involves public-key cryptography. The client establishes a public key/private key pair and provides the public key to the server. In a transaction, to prove its authenticity to the server, the client forms a digital signature with its private key on a time-varying message, and the server verifies the digital signature with the client's public key. The time-varying message, which may

be a timestamp or a challenge supplied by the server, is different in each instance. This message, when checked by the server, provides safeguards against a third party impersonating the client by simply replaying copies of previous signatures of the client that the third party has intercepted or otherwise acquired" [column 1 lines 24-36];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "the incorrect cryptographic key is identical in bit-length to the correct cryptographic key," in the invention as disclosed by Gennaro et al. and Collberg et al. for the purposes of providing safe guard against replay attacks.

10. Claims 32 & 37 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gennaro et al. (US-6317834-B1) in view of Collberg et al. (US-6668325-B1) and in further view of Chow et al. (US-6779114-B1).

Claim 32:

Gennaro et al. and Collberg et al. disclose a method of biometric verification using an access software application locally stored on a device and configured to access another application, system or other software entity on said device to protect biometric data against spoofing or theft, as in Claim 1 above, but their combination do not explicitly disclose,

- "the evaluation result comprises branching to a distinct location of the access software application if the user-provided biometric data is found to match the biometric template," although Chow et al. does suggest control flow encoding, as recited below;

however, Chow et al. does disclose,

- "Control-flow describes the manner in which execution progresses through the software code. The invention increases the complexity of the control flow by orders of magnitude, obscuring the flow of its algorithm and preventing the attacker from identifying and tampering with targeted areas" [column 6 lines 8-13];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "the evaluation result comprises branching to a distinct location of the access software application if the user-provided biometric data is found to match the biometric template," in the invention as disclosed by Gennaro et al. and Collberg et al. for the purposes of providing tamper resistance by control flow encoding.

Claim 37:

Gennaro et al. and Collberg et al. disclose a method of biometric verification using an access software application locally stored on a device and configured to access another application, system or other software entity on said device to protect biometric data against spoofing or theft, as in Claim 1 above, but their combination do not explicitly disclose,

- "the TRS encoding comprises mass data encoding for data in array, table or message buffer form," although Chow et al. does suggest mass data encoding, as recited below;

however, Chow et al. does disclose,

- "If a large number of control transfers are added to the software code, it will be extremely difficult for the attacker to identify the specific line of control that he wishes to modify" [column 12 lines 23-26];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "the TRS encoding comprises mass data encoding for data in array, table or message buffer form," in the invention as disclosed by Gennaro et al. and Collberg et al. for the purposes of providing tamper resistance by mass data encoding.

Response to Arguments

11. Applicant's arguments with respect to claims 1, 31-34, 36, & 37 have been considered but are moot in view of the new ground(s) of rejection.

Conclusion

12. The prior art made of record and not relied upon is considered pertinent to the applicant's disclosure.

a. Scheidt et al. (WO-2003065169) - access system utilizing multiple factor identification and authentication;

b. Forrest (US-20030088782-A1) - biometrics template;

c. Hamid (US-20030223624-A1) - method and apparatus for hashing data;

d. Hillhouse (US-20040005087-A1) - method and apparatus for supporting a biometric registration performed on an authentication server;

e. Borza (US-5995630) - biometric input with encryption;

f. Cromer et al. (US-20030070079-A1) - method and system for preboot user authentication;

2. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Examiner Oscar Louie whose telephone number is 571-270-1684. The examiner can normally be reached Monday through Thursday from 7:30 AM to 4:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami, can be reached at 571-272-4195. The fax phone number for Formal or Official faxes to Technology Center 2400 is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private

PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

OAL
08/12/2009

/Nasser G Moazzami/

Supervisory Patent Examiner, Art Unit 2436